HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Katharina Schönner

JTAG-Probing zur Datensicherung von Mobiltelefonen

2017

Fakultät: Computer- und Biowissenschaften

BACHELORARBEIT

JTAG-Probing zur Datensicherung von Mobiltelefonen

Autor/in:
Frau Katharina Schönner

Studiengang:
Allgemeine und digitale Forensik

Seminargruppe:
FO14w2-B

Erstprüfer:
Prof. Dr. Christian Hummert

Zweitprüfer:
Prof. Dr. Dirk Pawlaszczyk

Einreichung:
Mittweida, 22.09.2017

Faculty of Computer and Life Sciences

BACHELOR THESIS

JTAG-Probing to mirror the data of mobile phones

author:
Ms. Katharina Schönner

course of studies:
General and digital forensics

seminar group:
FO14w2-B

first examiner:
Prof. Dr. Christian Hummert

second examiner:
Prof. Dr. Dirk Pawlaszczyk

submission:
Mittweida, 22.09.2017

Bibliografische Angaben

Schönner, Katharina:

JTAG-Probing zur Datensicherung von Mobiltelefonen

JTAG-Probing to mirror the data of mobile phones

26 Seiten, Hochschule Mittweida, University of Applied Sciences,
Fakultät Medien, Bachelorarbeit, 2011

Abstract

Durch die steigende Bedeutung von Mobiltelefonen in Alltag- und Berufsleben nimmt auch, besonders aus forensischer Sicht, die Notwendigkeit einer korrekten Sicherung der hier zu gewinnenden Daten zu, im gleichen Maße wie die Vielseitigkeit und der Umfang dieser Daten. Im Rahmen der vorliegenden Arbeit wurde sich mit einer Möglichkeit der Identifizierung und Zuordnung von auf in Smartphones verbauten Platinen befindlicher JTAG Pins im Hinblick auf eine potentiell darauf folgende forensiche Datensicherung auseinandergesetzt. JTAG beschreibt einen seit 1990 gültigen Standard zum Testen und Debuggen von Hardware-Schaltungen auf Leiterplatten, ermöglicht aber auch das Programmieren und Debuggen von fest verbauten Prozessoren und FPGAs. Beim hierzu verwendeten Tool handelt es sich um die RIFF Box v2. Das hier auf Tauglichkeit zu prüfende Feature dieser Box konnte aufgrund eines technischen Fehlers, vermutlich eines Softwarefehlers seitens der RIFF Box, leider nicht getestet und das sogenannte Probing nicht durchgeführt werden.

Abstract

Due to the increasing meaning of mobile phones in daily and professional life, the necessity of forensic data extraction grows just like variety and amount of the backed up data. This paper deals with the possibility of identifying and assigning JTAG pins on mobile phones motherboards in order to be able to extract the data in a forensic way. JTAG was created 1990 and describes a standard for testing and debugging of embedded systems, but offers also the chance to debug and program integrated processors and FPGAs. The tool used for that trial was the so called RIFF Box v2, a JTAG flasher tool. Unfortunately the JTAG probing feature the box offers couldn´t be tested because of a technical error, probably a RIFF Box software issue.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Mit der zunehmenden Bedeutung von Mobiltelefonen im Alltagsleben steigen sowohl die Notwendigkeit, die dort gespeicherten Daten forensisch zu sichern und auszuwerten sowie auch der damit erzielte Erkenntnisgewinn. Anhand dieser Informationen sind zahlreiche Rückschlüsse über den Nutzer des betreffenden Gerätes möglich, beispielsweise auf seine Identität, sein Geschlecht und seine Gewohnheiten, unter Umständen auch auf seinen Gesundheitszustand oder seine religiösen Ansichten.[1] Ein Smartphone kann so vielfältige persönliche Informationen enthalten, dass eine Untersuchung nicht nur ein deutliches Bild des privaten Lebens des Nutzers, sondern auch seines Charakters ergeben kann, gerade durch die zunehmende Verwendung solcher Geräte zur Kommunikation.[2] Für forensische Untersuchungen gilt es dadurch auch, ein besonderes Augenmerk auf datenschutzrechtliche Aspekte zu legen, beispielsweise bei Ermittlungen in Unternehmen, da Smartphones häufiger als Computer betrieblich und privat genutzt werden.[3] Flash-Speicher sind hitze- und druckbeständiger als eine übliche Festplatte, was das Zerstören der Daten auf diesen erschwert.[4] Die RIFF Box ist ein Flasher Tool, das in erster Linie zu Reparaturzwecken für Smartphones verwendet wird. Sie kann allerdings auch zur Erstellung eines physikalischen Abbilds des Flashspeichers dieser Geräte eingesetzt werden. Dieses Image wird im Binär-Format (.bin) abgelegt, um es für die forensische Auswertung, beispielsweise mit EnCase oder XWays Forensics, ins Evidence-Witness-Format (.E01) zu konvertieren, benötigt man weitere Software, wie zum Beispiel den kostenlosen FTK Imager. Hash-Werte ändern sich bei einem solchen Vorgang nicht.[5] Physikalische Sicherung bedeutet, dass der Speicher tatsächlich bitweise, statt wie bei einer logischen Sicherung dateiweise, kopiert wird. Es werden also tatsächlich alle vorhandenen Spuren, auch gelöschte oder verborgene Dateien, gesichert. Bedenkt man den eigentlichen Hauptverwendungszweck der RIFF Box, wird deutlich, dass unter Umständen auch defekte Geräte auf diese Art gesichert werden können, solange zum Beispiel nur der Bootloader beschädigt ist. Im Vergleich zu anderen Methoden ist die Verwendung von JTAG, wie in Abbildung 3 zu sehen ist, ein ausgewogener Mittelweg zwischen Datenintegrität und Risiko. Bei Chip-off-Forensik zum Beispiel

[1] vgl. Mylonas, Alexios: Security and Privacy in Ubiquitous Computing: The Smart Mobile Equipment Case, 2013, S.1ff

[2] vgl. Mylonas et al.: Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition, 2011, S.254

[3] vgl. Schonschek, Oliver: Digitale Spurensuche auf Smartphones: Tools für die mobile Forensik, 2013, URL: https://www.computerwoche.de/a/tools-fuer-die-mobile-forensik,2533050, 11.09.2017

[4] vgl. Kong, Yu Cho: A Forensic Analysis Approach to Smartphones from a criminal investigation perspektive, 2015, S.3f

[5] vgl. https://articles.forensicfocus.com/2014/03/11/jtag-sch-r530u-that-has-android-4-3-on-it/, 22.08.2016

besteht das Risiko, den Speicherchip durch die beim Ablöten entstehende Hitze zu beschädigen, dafür bleibt das Zielgerät durchgehend ausgeschaltet, so dass es hier nicht zu Veränderungen der Daten kommen kann.[6] Dieses Vorgehen ist vor allem bei defekten Zielgeräten anzuwenden, da es auch dann oft zum Erfolg führt und zudem irreparable Schäden am Smartphone herbeiführt.[7] Die in Abbildung 3 ebenfalls genannte Bootloader Methode beschreibt die Möglichkeit, zumindest bei Windows Mobiles von HTC mittels der USB-Schnittstelle des Smartphones ein Abbild zu erstellen. Diese Möglichkeit besteht hier, da der in diesem Modell verwendete Bootloader neben den üblichen Fähigkeiten zum Update und der Prüfung der Hardware auch für Diagnose und Wartung verwendet wird.[8] Damit ist dieses Vorgehen weitaus weniger häufig anwendbar und nicht als forensiches Standardvorgehen anzusehen. Diese drei Methoden entsprechen einer physikalischen Datensicherung, im Vergleich dazu liefert eine logische Sicherung grundsätzlich weniger Informationen,[9] zudem werden die Daten wie bereits erwähnt zur Laufzeit des Systems mittels entsprechender Software gesichert, was eine gewisse Gefährdung der Datenintegrität zur Folge hat.[10] Aufgrund dieser Differenz im Beweisgehalt der Methoden kamen vier Wissenschaftler 2007 zu dem Schluss, dass die Verwendung von JTAG die am stärksten zu empfehlende Methode sei.[11]

[6] vgl. Breeuwsma, Marcel et al.: Forensic Data Recovery from Flash Memory, 2007, S.7

[7] vgl. Muth, Denise: Leitfaden zur forensischen Untersuchung von Android-Smartphones, 2013, S.63, URL: https://www.dasec.h-da.de/wp-content/uploads/2013/08/muth-denise-masterarbeit-ss131.pdf, 05.10.2016

[8] vgl. Yung Anh Le:Windows Phone 7 : Implications For Digital Forensic Investigators, 2012, S.34f

[9] vgl. Yung Anh Le:Windows Phone 7 : Implications For Digital Forensic Investigators, 2012, S.40

[10] vgl. Kong, Yu Cho: A Forensic Analysis Approach to Smartphones from a criminal investigation perspektive, 2015, S.12

[11] vgl. Keonwoo Kim, Dowon Hong, Kyoil Chung, and Jae-Cheol Ryou: Data Acquisition from Cell Phone using Logical Approach, in: Proceedings of world academy of science, engineering and technology, 2007, S.32

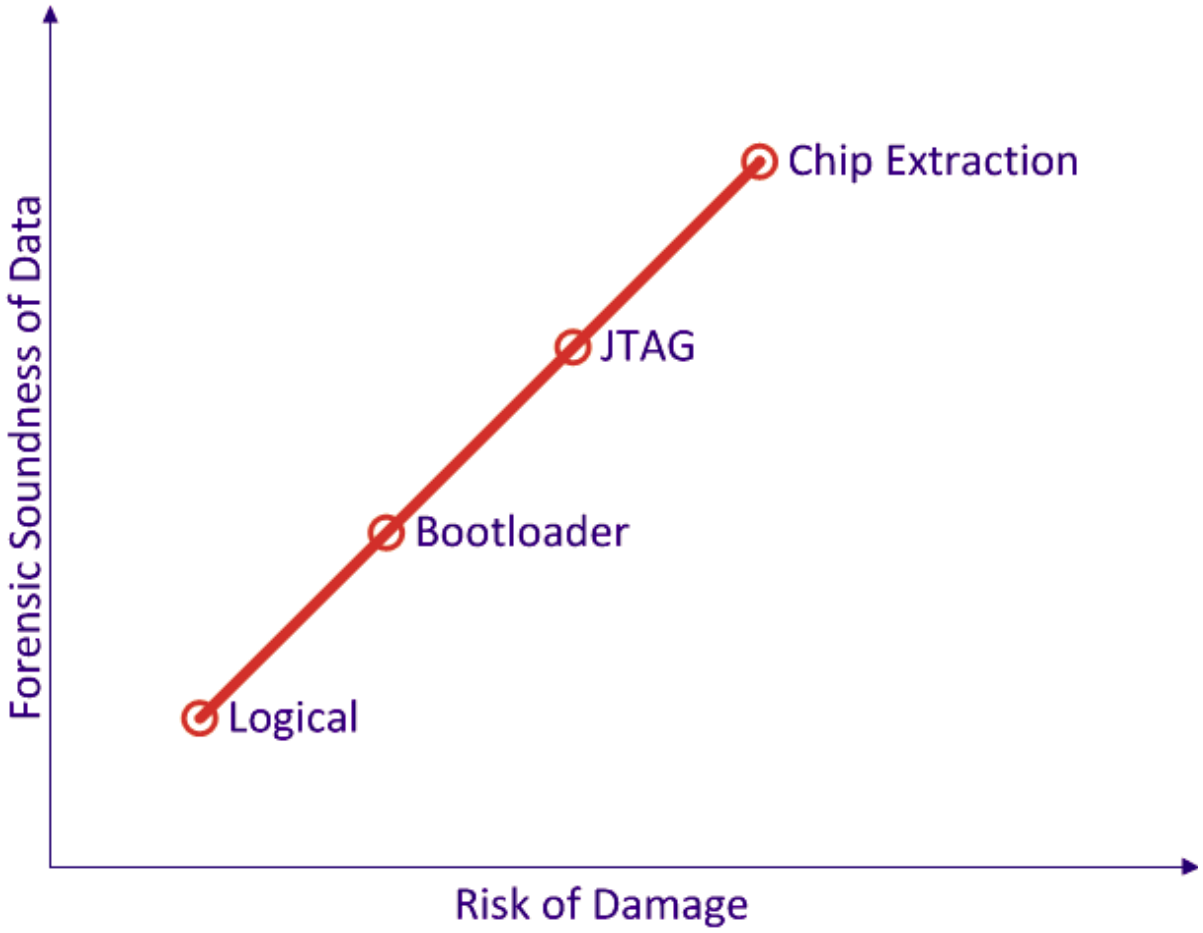

Abbildung 1 Einstufung des Risikos unterschiedlicher Methoden zur Datensicherung[12]

Die RIFF Box arbeitet, wie bereits erwähnt, über JTAG, eigentlich Joint Test Action Group, ein Begriff, der häufig als Synonym für den Standard IEEE 1149.1 verwendet wird. Dieses Verfahren besteht seit 1990 und wird verwendet, um integrierte Hardware auf Leiterplatten zu testen. Durch die Zunahme an Funktionalität einzelner Systeme steigt auch der Bedarf, einzelne integrierte Komponenten oder das System im Ganzen zu testen. Gleichzeitig sind diese Bestandteile heute in Geräten aber nur schwer zugänglich, was die Testmöglichkeiten eingrenzt.

[12] Yung Anh Le:Windows Phone 7 : Implications For Digital Forensic Investigators, 2012, S.37

Als Lösung wurden virtuelle Testpunkte in die Hardware eingebaut, die über die JTAG Schnittstelle statt über physische Verbindungen erreicht werden und deren Protokoll um nutzer- und herstellerspezifische Befehle erweitert werden kann. [13] Das seriell und synchron realisierte[14] JTAG Interface, insgesamt auch Test Access Port (TAP) genannt, ist an einen Zustandsautomaten (TAP-Controller) gekoppelt[15] und nutzt die vier Hauptsignale

TCK – Test Clock: Taktung der Schnittstelle

TMS – Test Mode Select: Navigation im Zustandsautomaten

TDI – Test Data Input: Datenübertragung zum Gerät hin

TDO – Test Data Output: Datenleitung vom Gerät weg

Und im Falle der RIFF Box folgende weitere Signale:

TRST: Test Reset[16]: Versetzung der Schnittstelle in einen definierten Ausgangszustand

NRST: Reset der gesamten Geräte-Hardware

---

[13] Vgl. Günther, Stephan: JTAG-Interface, Überblick über Aufbau, Funktion und Nutzung, URL: https://tu-dresden.de/ing/informatik/ti/vlsi/ressourcen/dateien/dateien_studium/dateien_lehstuhlseminar/vortraege_lehrstuhlseminar/hs_ws_0708/jtag-schnittstelle.pdf?lang=de, 10.09.2017

[14] vgl. Heinz, Benedikt : Hardware-Debugschnittstelle JTAG auslesen, Linux-Magazin, 2010, URL: http://www.linux-magazin.de/Ausgaben/2010/06/Diagnosewerkzeug, 23.07.2017

[15] vgl. Heinz, Benedikt : Hardware-Debugschnittstelle JTAG auslesen, Linux-Magazin, 2010, URL: http://www.linux-magazin.de/Ausgaben/2010/06/Diagnosewerkzeug, 23.07.2017

[16] vgl. Günther, Stephan: JTAG-Interface, Überblick über Aufbau, Funktion und Nutzung, URL: https://tu-dresden.de/ing/informatik/ti/vlsi/ressourcen/dateien/dateien_studium/dateien_lehstuhlseminar/vortraege_lehrstuhlseminar/hs_ws_0708/jtag-schnittstelle.pdf?lang=de, 10.09.2017 und
Technical Guide to JTAG, URL: https://www.xjtag.com/about-jtag/jtag-a-technical-overview/, 19.07.2017

RTCK – returned clock (optional): Synchronisierung mit der Laufzeit-Uhr des Geräts

Dabei folgt JTAG dem Protokoll, das in Abbildung 2 dargestellt ist.

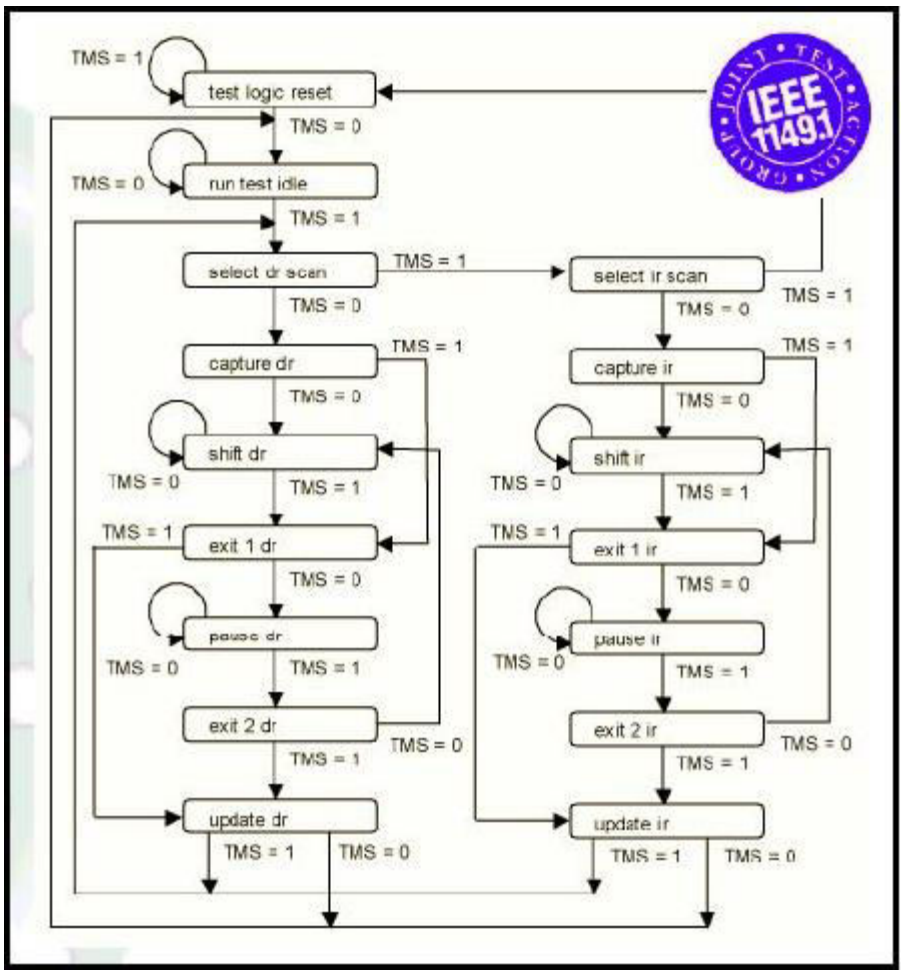

Abbildung 2 JTAG Protokoll, Verhalten des TAP Controllers in Abhängigkeit der eingehenden TMS-Daten[17]

[17] Günther, Stephan: JTAG-Interface, Überblick über Aufbau, Funktion und Nutzung, URL: https://tu-dresden.de/ing/informatik/ti/vlsi/ressourcen/dateien/dateien_studium/dateien_lehstuhlseminar/vortraege_lehrstuhlseminar/hs_ws_0708/jtag-schnittstelle.pdf?lang=de, 10.09.2017 S.7

Wie in Abbildung 2 beschrieben, werden in Abhängigkeit vom vorherigen Zustand des Automaten und der eingehenden TMS-Daten, nach TCK getaktet, unterschiedliche Aktionen ausgeführt.[18] Dabei steht „ir“ für „instruction register“ und „dr“ für „data register“, das aus denjenigen Registern besteht, die an der Übertragung von Nutzdaten beteiligt sind.[19] Unterschiedlich viele JTAG-Bausteine, die jeweils einen TAP Controller besitzen, bilden in JTAG-fähigen Geräten eine JTAG-Kette, so dass bei einer Schiebeoperation Daten am TDI ins Register des jeweiligen Bauteils hinein- beziehungsweise am TDO desselben hinaus- und über TDI wieder in den nächsten Baustein hineingeleitet werden (siehe Abbildung 3).

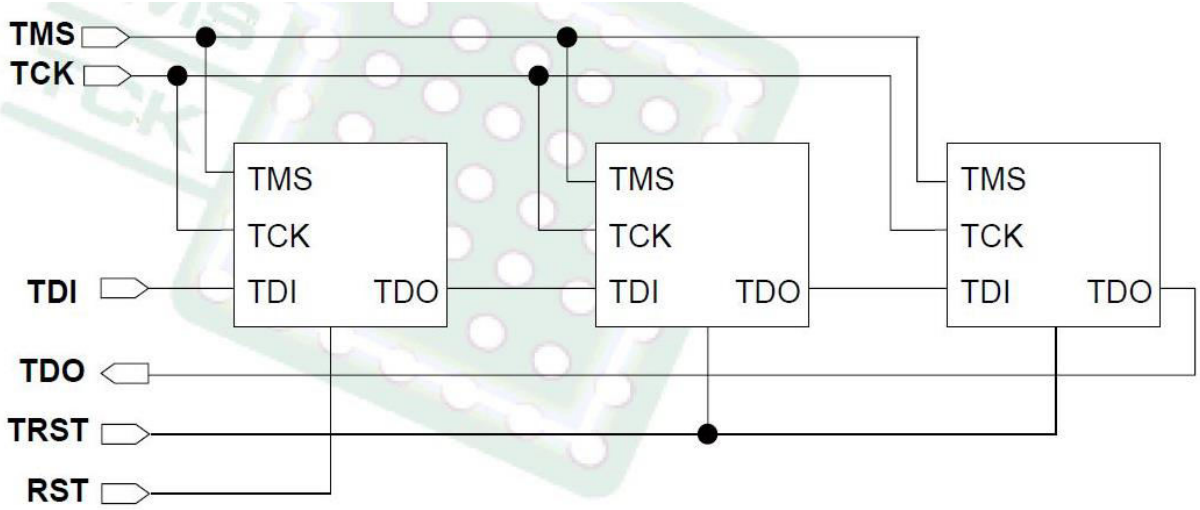

Abbildung 3 JTAG-Chain[20]

[18] vgl. Günther, Stephan: JTAG-Interface, Überblick über Aufbau, Funktion und Nutzung, URL: https://tu-dresden.de/ing/informatik/ti/vlsi/ressourcen/dateien/dateien_studium/dateien_lehstuhlseminar/vortraege_lehrstuhlseminar/hs_ws_0708/jtag-schnittstelle.pdf?lang=de, 10.09.2017, S.42 und
vgl. Domke, Felix: Blackbox JTAG Reverse Engineering, 2009

[19] vgl. https://www.xjtag.com/about-jtag/jtag-a-technical-overview/,

[20] Günther, Stephan: JTAG-Interface, Überblick über Aufbau, Funktion und Nutzung, URL: https://tu-dresden.de/ing/informatik/ti/vlsi/ressourcen/dateien/dateien_studium/dateien_lehstuhlseminar/vortraege_lehrstuhlseminar/hs_ws_0708/jtag-schnittstelle.pdf?lang=de, 10.09.2017 S.17

Grundsätzlich sind Flash-Speicherchips nicht immer JTAG-fähig, aber für gewöhnlich mit anderen Chips, wie Prozessoren, verbunden, über die ein solcher Zugriff dann erfolgen kann.[21] JTAG liefert die Möglichkeit, auf zwei Arten mit der Hardware des Geräts zu kommunizieren. Es erlaubt das Lesen bzw Schreiben des Speichers und das Ausführen von Code für den Mikroprozessor (MCU).[22] Da es allerdings keine einheitliche Steckerbelegung für JTAG-Anschlüsse gibt, muss vorab die Pinbelegung je nach Model in Erfahrung gebracht werden.[23]

Eine mögliche Hilfe dabei kann die RIFF Box sein. Das Tool besteht im Wesentlichen aus der Hardware RIFF Box und der Software JTAG Manager. Die RIFF Box unterstützt eine Vielzahl an Modellen (darunter viele Samsung Geräte, Alcatel Modelle, Geräte von Haier, HTC, Huawei, LG, MicroMax, Motorola, Nokia, Pantech, Sony Ericsson, Sierra, Toshiba, ZTE und vereinzelte andere) und kann seit Version v1.58 (April 2016, bereits veraltet) auch eMMCs auslesen. Sollte ein Gerät von der RIFF BOX nicht unterstützt sein, kann ein technisch versierter Nutzer mittels der Lauterbach Testsprache PRACTICE über die Option JTAG Read/Write auch das abdecken.[24] Am 09.08.16 wurde eine neue Hardware-Version der RIFF Box herausgegeben, die voll kompatibel mit Windows 10 ist. Sie verfügt außerdem im Gegensatz zur vorigen Version über eine USB-Schnittstelle und installiert beim Anschließen an ein Gerät mit Windows 10 automatisch alle benötigte Software, diese wurde um den RIFF Remote helper, den RIFF Admin client / SN reader und RIFF Box USB Treiber erweitert.

Beim hier zum Testen verwendeten Smartphone handelt es sich um ein Sony Xperia T (LT30p) mit Qualcomm Krait MSM8260-A Dual-Core-Prozessor, 4,6 Zoll Touchscreen, 1GB RAM, 1,5 GHz und 13 Megapixel Kamera, das James Bond Phone in „Skyfall“.[25] Die RIFF Box unterstützt zwar den Prozesor, nicht aber das Modell.[26]

---

[21] vgl. Breeuwsma, Marcel et al.: Forensic Data Recovery from Flash Memory, 2007, S.4

[22] vgl. RIFF Box Getting Started, URL: https://www.riffbox.org/category/jtag-support/, 27.06.2017

[23] vgl. Heinz, Benedikt : Hardware-Debugschnittstelle JTAG auslesen, Linux-Magazin, 2010, URL: http://www.linux-magazin.de/Ausgaben/2010/06/Diagnosewerkzeug, 23.07.2017

[24] vgl. RIFF Box User Manual, URL: https://www.riffbox.org/category/jtag-support/, 27.06.2017

[25] vgl. Heinfling, Benjamin: Ice Cream Sandwich statt Wodka Martini, 2012, URL: http://www.chip.de/artikel/Sony-Xperia_T-Handy-Test_57975160.html , 05.07.2017

[26] vgl. RIFF JTAG Features, URL : http://www.riffbox.org/category/riff-jtag-features/, 17.04.2017

2 Methoden

Das hier untersuchte Feature der RIFF Box, das Probing, soll es dem Nutzer laut Hersteller ermöglichen, die JTAG Pins eines nicht unterstützten Modells korrekt zuzuordnen. Auch kann damit festgestellt werden, ob es sich bei einer Anordnung von Pins auf einem Motherboard tatsächlich um eine JTAG Schnittstelle handelt. Dazu wird mit einer Nadel an jedem Pin die Spannung am ADC2 Punkt bei einem PRB_LEVEL Signal beim logischen Null-Level (Probe(0), V1) und einem PRB_LEVEL Signal beim logischen Eins-Level (Probe(1), V2) gemessen (siehe Abbildung 4).

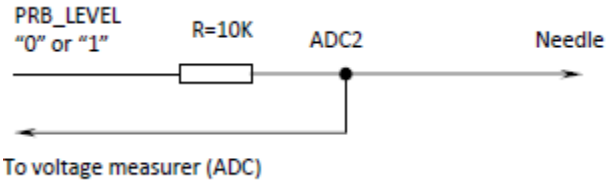

Abbildung 4 Aufbau des Probing[27]

Durch den bereits in der Box verbauten 10k Ohm Widerstand wird bei den verwendeten 2.6V Differenz (für Qualcomm-Prozessoren, in Tabelle 1 die ersten sechs Modelle[28]) zwischen den logischen Leveln nur eine Stromstärke von etwa 0.25 mA erreicht. Deswegen ist diese Methode laut der Hersteller sicherer als Pinfinder Lösungen, da der Widerstand eventuelle Schäden am Gerät verhindert.[29]

Von den Herstellern empfohlenes Vorgehen:[30]

1) Messung der Spannung auf den zu identifizierenden Pads mittels eines Multitesters
2) Entsprechende Einstellung der Spannung in der JTAG Manager Software im JTAG I/O Voltage Feld in den Custom Target Settings
3) Klicken des Start Probing Buttons
4) Wählen des PAD Type Sensor Mode

[27] RIFF Box Probing Manual, URL :
http://www.riffbox.org/downloads/manuals/JTAG_Signals_Probing.pdf, 2010
[28] vgl. ebd.
[29] vgl. ebd.
[30] vgl. ebd.

5) Für eine möglichst genaue Messung das GND Signal des RJ-45 Anschlusses der RIFF Box mit dem Gerät verbinden
6) Die Pads auf dem Motherboard des Handys mit der zum Probing verwendeten Nadel berühren
7) Durch Logik oder angezeigte Hilfestellungen die Ergebnisse korrekt interpretieren
8) Wenn TRST, RTCK und TDO mit hoher Wahrscheinlichkeit korrekt zugeordnet sind, müssen TDI, TMS und TCK, die die selben Parameter aufweisen, manuell bestimmt werden.
   8a) TRST, GND, RTCK und TDO werden an den JTAG Connector gelötet und an die RIFF Box angeschlossen
   8b) Aus den restlichen drei Pins (TDI, TCK, TMS) eines auswählen und mit dem TCK Signal an der RIFF Box verbinden.
   8c) Zum Überprüfen dieser Wahl Analize JTAG Chain klicken, falls die Zuordnung korrekt war, wird None Found als Fehler angezeigt, andernfalls RTCK does not respond. In höchstens drei Versuchen muss TCK gefunden werden.
   8d) Nach gleichem Vorgehen werden die übrigen zwei Signale zugeordnet.

Für das Huawei C2806M beispielsweise wurden auf diesem Wege folgende Werte ermittelt (siehe Tabelle 1):

Das TRST Signal lieferte für V1 den Wert 0,00V und für V2 2,27V.
Der Wert bei Probe(1), also V2, ist mit 2,27V eindeutig niedriger als die angelegte Spannung von 2.6V. Das ist durch den Spannungsabfall am Widerstand bedingt und zeigt, dass das TRST Signal Input ist und mit keinem Pull-Up-Widerstand irgendwo auf dem Board verbunden ist.[31]
Wie bereits erwähnt liefern TDI, TMS und TCK die selben Parameter, in diesem Fall für Probe(0) einen Wert von 0,31V und für Probe(1) 2,59V. Obwohl also bei V1 die Spannung auf Null gesetzt ist, ist sie hier wesentlich höher. Das ist dem Pull-Up-Widerstand geschuldet, der mit dem TDI, TMS und TCK Signal auf dem Board verbunden ist. Auch am bei V2 ermittelten Wert von 2,59 wird deutlich, dass die Spannung hier im Gegensatz zum TRST Signal nicht abfällt.
Das RTCK Signal wies bei Probe(0) eine Spannung von 0,08V und bei Probe(1) eine von 0,09V auf. Hier ändert sich also die resultierende nicht durch die angesetzte Spannung von 0,00V bzw. 2,6V. Also ist das RTCK Signal ein Output Signal, das im logischen null Level verbleibt.
Das TDO Signal befindet sich für gewöhnlich im Z-State, deswegen wurde für Probe(0) ein Wert von 0,00V und für Probe(1) einer von 2,60V gemessen. Im Z-State fließt kein

[31] *Pull-up* bezeichnet in der Elektrotechnik einen (relativ hochohmigen) Widerstand, der eine Signalleitung mit dem höheren Spannungs-Potential verbindet. Durch ihn wird die Leitung auf das höhere Potential gebracht, für den Fall, dass kein Ausgang die Leitung *aktiv* auf ein niedrigeres Potential bringt. Übliche Werte liegen im Bereich von 1 kΩ bis rund 10 kΩ
https://de.wikipedia.org/wiki/Open_circuit#Pull-up, 18.05.2017

Strom, also kommt es nicht zu einem Spannungsabfall. Das TDO Signal verhält sich dadurch wie ein Input Signal mit sehr großem Eingangswiderstand.
Das NRST Signal ergab für V1 eine Spannung von 1,45V und für V2 2,62V.
Der hohe Wert bei Probe(0), der dennoch eindeutig unter der bei Probe(1) verwendeten Spannung liegt, bedeutet, dass ein recht starker Pull-Up-Widerstand verwendet wird, um das NRST Signal zu erhöhen.[32]
Bei den Modellen Samsung B7330 oder S5230 ist für das NRST Signal kein klarer Unterschied zwischen Input und Output Mode erkennbar. Das bedeutet, dass der verwendete 10K Widerstand so groß ist, dass ein so starker Pull-Up-Widerstand wie er bei diesen Geräten für das NRST Signal verwendet wird die Zuweisung als Input Pin mit Pull-Up oder als Output Pin im logischen Status Eins verhindert.
In Tabelle 1 sind die jeweiligen gemessenen Spannungen für diverse Modelle eingetragen, ein „+C“ hinter dem Modelnamen bedeutet, dass das Gerät während der Messungen per USB Kabel an einen Laptop angeschlossen war, ein „+B“, dass sich die Batterie währenddessen im Gerät befand. Die Spannungen sind jeweils in Volt angegeben, der erstgenannte Wert bezeichnet dabei die gemessene Spannung bei V1, der zweite analog bei V2.

Tabelle 1 Ergebnisse des Probing für verschiedene Modelle[33]

Model	MCU	TRST	TDI	TMS	TCK	RTCK	TDO	NRST
HTC HD2 + C + B	QSD8250	0.13/2.11	0.29/2.64	0.29/2.64	0.29/2.64	0.14/0.15	0.00/2.61	1.45/2.62
HTC HD + C	MSM7201A	0.00/2.25	0.31/2.59	0.31/2.59	0.31/2.59	0.00/0.00	0.00/2.60	1.35/2.62
HTC HD + C + B	MSM7201A	0.01/2.27	0.30/2.63	0.30/2.63	0.30/2.63	0.08/0.09	0.00/2.60	1.38/2.65
Huawei C2806M + C	QSC6010	0.00/2.28	0.37/2.59	0.37/2.59	0.37/2.59	0.00/0.00	0.00/2.60	1.23/2.57
Samsung B7330 + C + B	MSM7225	0.01/2.24	0.32/2.62	0.32/2.62	0.32/2.62	0.03/0.04	0.00/2.60	2.64/2.66
Samsung U700	MSM6280	0.00/2.26	0.32/2.60	0.32/2.60	0.32/2.60	0.00/0.00	0.00/2.60	1.23/2.60

[32] vgl. RIFF Box Probing Manual, URL :
http://www.riffbox.org/downloads/manuals/JTAG_Signals_Probing.pdf, 2010

[33] RIFF Box Probing Manual, URL :
http://www.riffbox.org/downloads/manuals/JTAG_Signals_Probing.pdf, 2010

Samsung I9000	S5PC110	0.05/2.34	0.37/2.86	0.37/2.86	0.05/2.35	-	0.01/2.80	0.37/2.85
Samsung i900 PDA + C	PXA312	1.92/3.30	0.34/3.30	0.34/3.30	0.05/1.65	-	0.00/3.28	0.44/3.26
Samsung S5230 + C	BCM2133x	0.00/1.89	1.37/2.96	1.37/2.96	0.00/1.88	0.00/0.00	0.27/2.97	2.93/2.95

Um dieses Verfahren nun zu testen, wurde zunächst ein System mit Windows 7 Home Premium verwendet. Dabei kam es hier im Geräte-Manager zu einem Fehlercode 10, für den der Hersteller bereits eine Anleitung zur Behebung auf der Homepage veröffentlicht hat.[34]

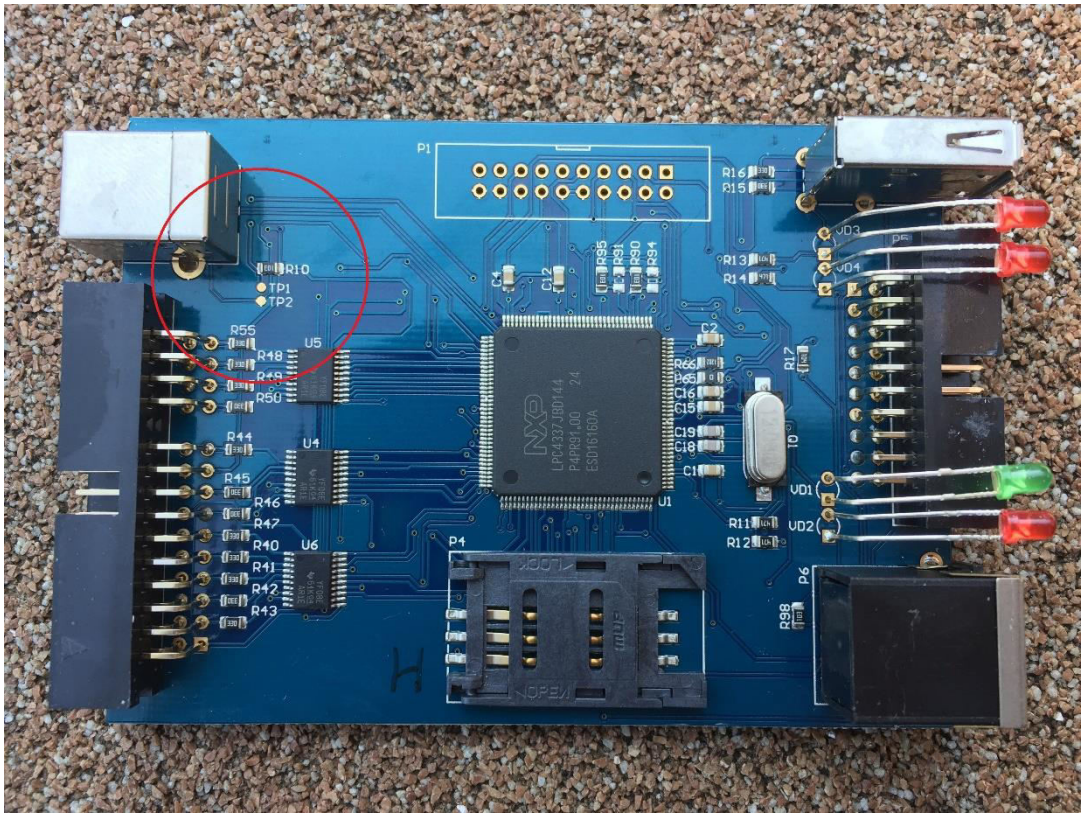

Abbildung 5 Hardware RIFF Box zerlegt[35]

[34] vgl. RIFF JTAG Manager v1.67, RIFF Box Firmware v1.43, 2017, URL: https://www.riffbox.org/jtag-news/riff-jtag-manager-v1-67-riff-box-firmware-v1-43/, 19.04.2017

[35] http://www.riffbox.org/wp-content/uploads/2017/04/TP.jpg, 24.04.2017

Laut dieser soll man während des Anschließens der Box an den PC per USB die Testpoints (TP1, TP2, siehe Abbildung 5) mit einer Pinzette verbinden.[36]

Um das zum Probing verwendete System möglichst auch weiterhin einsatzbereit weitergeben zu können, wurde dafür stattdessen eine virtuelle Maschine mit Widows 10 Home auf bereits genanntem Hostsystem eingerichtet.
Aufgrund fehlender Hardwarebeschleunigung zur Virtualisierung (gebraucht wurde ein Lifebook mit Intel® Pentium® CPU P6200 Prozessor ohne Virtualisierungstechnik)[37] konnte Oracles VirtualBox nicht von der verwendeten ISO-Datei booten, daher wurde der kostenlose VMware Workstation Player genutzt. Die virtuellen Maschinen lassen sich hiermit später in eine OVA/OVF Datei umwandeln, die wiederum nach VirtualBox importiert können werden sollte.[38]
Zwar können diese unter VMware nur als OVF exportiert werden, während VirtualBox OVAs erstellt, aber da sich beide Formate lediglich in der Art des Ablegens (OVA alles in einer Datei, OVF als Disk-Image plus Beschreibung der Maschine)[39] unterscheiden, ist ein Importieren zwischen beiden Virtualisierungssoftware-Versionen möglich.
Nach der Installation und Einrichtung von Windows 10 musste die zur Verwendung der RIFF Box nötige Software „JTAG Manager“ von der Website der Hersteller heruntergeladen und anschließend über den Gerätemanager die erforderlichen Treiber installiert werden.
Die RIFF Box kann nach Registrierung (Angabe einer E-Mail Adresse, Setzen eines Nutzernamens und eines Passworts) verwendet werden.
Da für das Probing der RJ-45 Ausgang der RIFF Box genutzt wird (siehe Abbildung 6), bietet sich, besonders für Nutzer ohne Löt-Kenntnisse, die Verwendung eines speziell dafür entwickelten RIFF Probe Kabels[40] an, wodurch das Löten vermieden werden kann. Allerdings muss dann insofern von der Anleitung der Hersteller abgewichen werden, dass ein GND Pin am JTAG Interface der RIFF Box anstelle des GNDs am RJ-45 Ausgang genutzt wird. Der zum Probing verwendete Aufbau ist in Abbildung 7 skizziert.

[36] vgl. RIFF JTAG Manager v1.67, RIFF Box Firmware v1.43, 2017, URL: https://www.riffbox.org/jtag-news/riff-jtag-manager-v1-67-riff-box-firmware-v1-43/, 20.04.2017

[37] vgl. http://ark.intel.com/de/products/50176/Intel-Pentium-Processor-P6200-3M-Cache-2_13-GHz, 13.05.2017

[38] vgl. Hoffman, Chris: How To Convert Virtual Machines Between VirtualBox and Vmware, 2012, URL: https://www.howtogeek.com/125640/how-to-convert-virtual-machines-between-virtualbox-and-vmware/, 07.06.2017

[39] vgl. http://www.askingbox.de/frage/virtualbox-unterschied-zwischen-ova-und-ovf-datei, 15.06.2017

[40] vgl. https://www.fonefunshop.com/Probe-Cable-For-Riff-Box.html, 05.08.2017

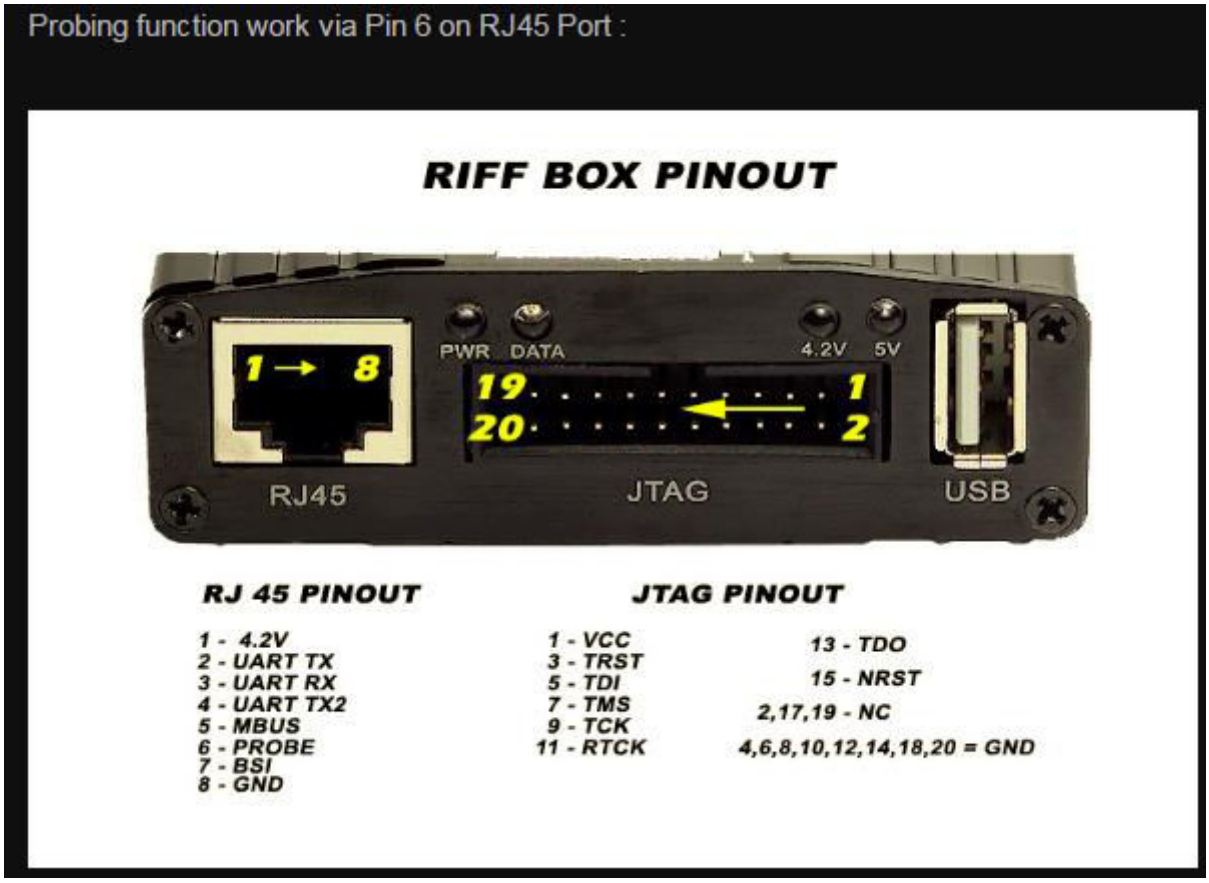

Abbildung 6 Pinout der RIFF Box[41]

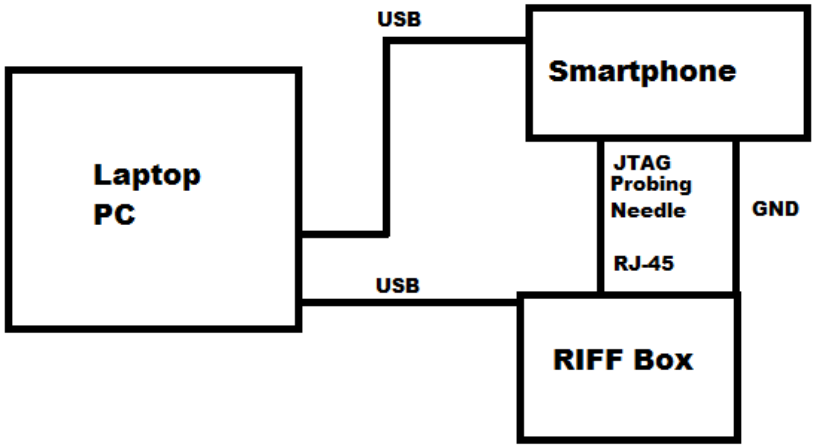

Abbildung 7 Aufbau zum Probing (Skizze)

[41] https://www.riffbox.org/tag/pins/, 16.07.2017

Nun muss das zum Testen des Features verwentete Smartphone soweit zerlegt werden, dass man problemlosen Zugriff auf das Motherboard, auf dem sich die JTAG Pins befinden, hat.
Zunächst wird dafür die Abdeckung der Steckplätze für SIM- und micro SD-Karte geöffnet und die dort befindliche Schraube entfernt. Nun lässt sich die hintere Abdeckung bereits abnehmen.[42]
Dann müssen die Steckverbindungen über dem Akku gelöst werden, darunter befinden sich JTAG Pins (siehe Abbildung 8).

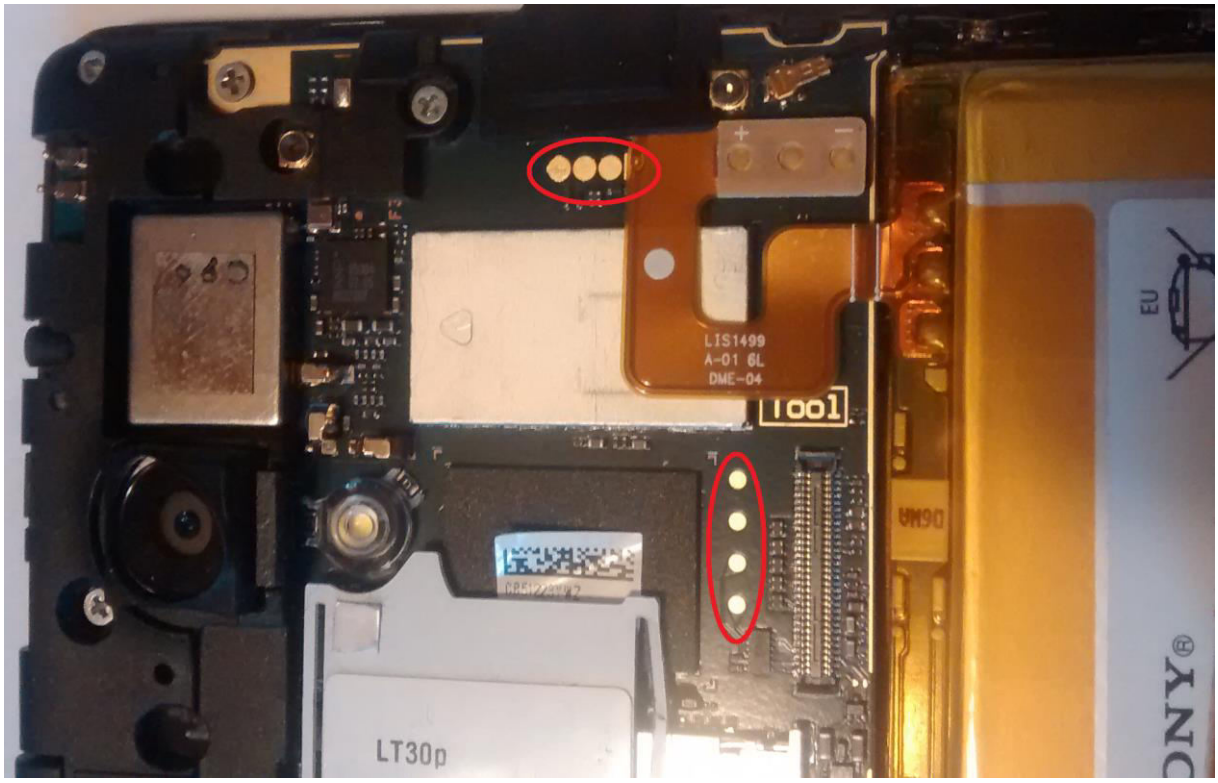

Abbildung 8 Sony Xperia T LT30p zerlegt, vermutete JTAG Pins hervorgehoben

[42] vgl. https://www.youtube.com/watch?v=4BtXZiVLtWc, 03.06.2017

3 Ergebnisse

Im hier verwendeten Sony Xperia T LT30p ist ein Qualcomm Prozessor mit einem Spannungsunterschied von 1,8 Volt verbaut.
Das Probing selbst konnte aufgrund technischer Probleme nicht durchgeführt werden.

Wird der Start Probing Button gedrückt, erscheint das gewünschte Fenster, es werden allerdings durchgehend die gleichen nicht nachvollziehbaren Werte angezeigt (siehe Abbildung 9 und 10).

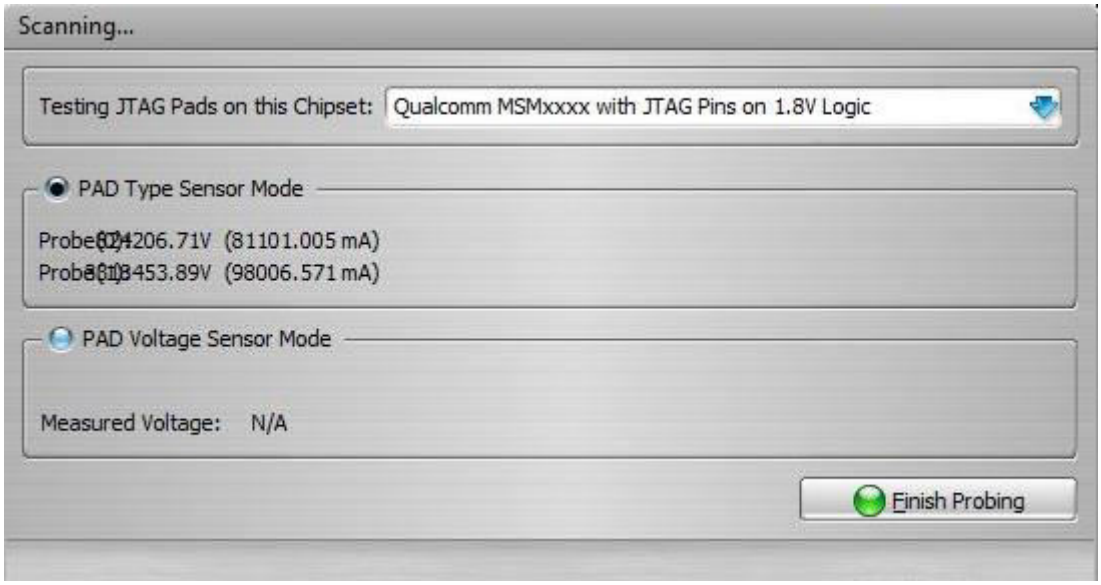

Abbildung 9 Anzeige beim Probing (Screenshot)

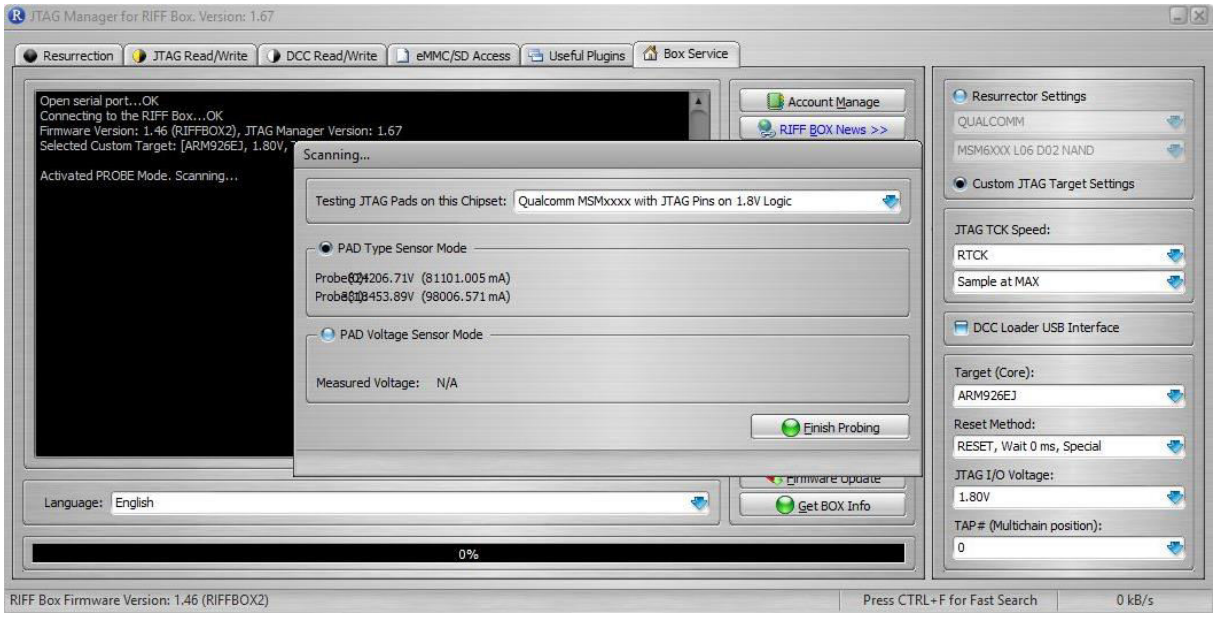

Abbildung 10 Anzeige Probing mit Einstellungen (Screenshot)

Gewünscht wäre bei Berühren eines Pads mit der Nadel eine Anzeige wie in Abbildung 11 beziehungsweise Abbildung 12.

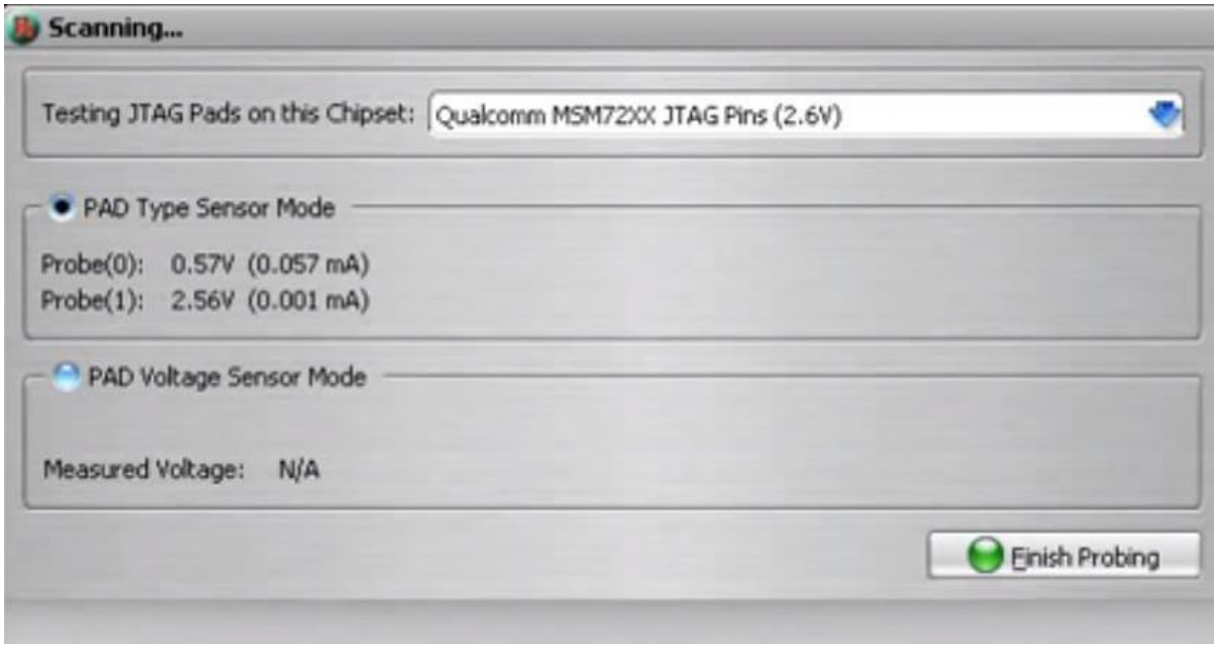

Abbildung 11 JTAGManager beim Probing PAD Type Sensor Mode[43]

[43] https://www.youtube.com/watch?v=luRdICkdkx8, 09.09.2017

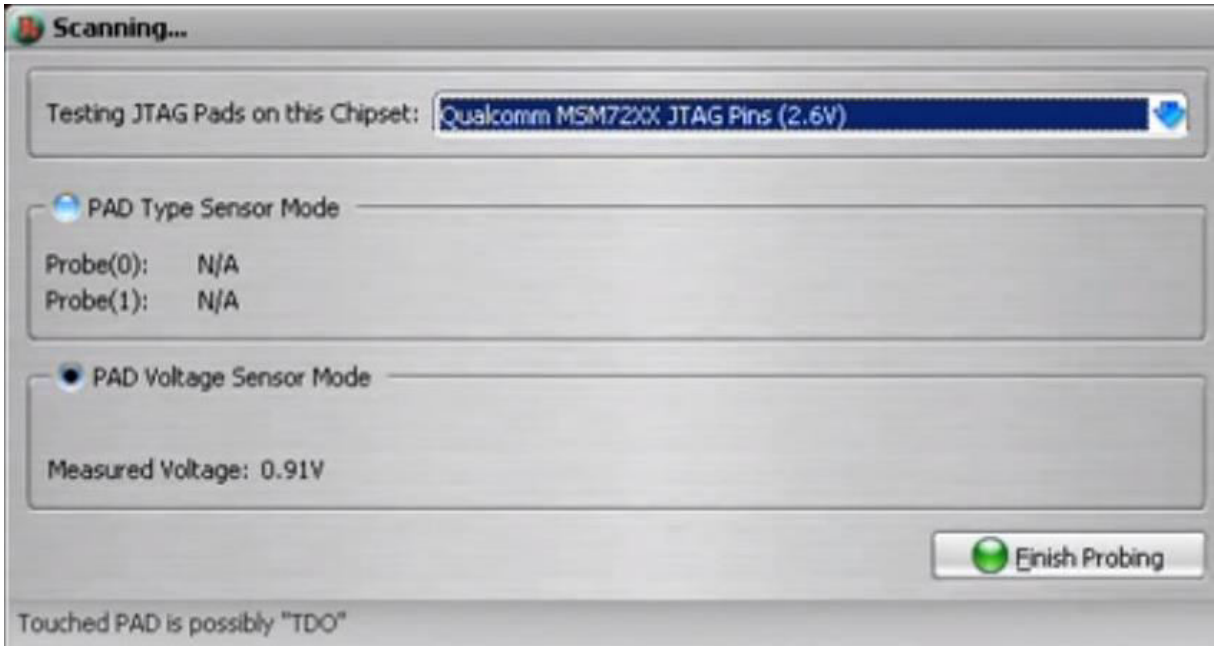

Abbildung 12 JTAGManager beim Probing PAD Voltage Sensor Mode mit Pin-Belegungsvorschlag[44]

[44] ebd.

4 Diskussion

Zunächst bestand die Möglichkeit eines Fehlers am Endgerät, also dem Smartphone.
Da auch die Verwendung eines anderen Sony Xperia T LT30p kein anderes Resultat erbrachte, war die erste Maßnahme die dahingehende Anpassung des Aufbaus, dass das Smartphone direkt an eine externe Stromversorgung statt dazu nur an den verwendeten Laptop angeschlossen wurde. Leider erzielte das weder im Verhalten des Smartphones noch dem der Software eine Änderung.
Deswegen wurde selbiges Vorgehen zusätzlich mit einem Sony Xperia Neo MT15i durchgeführt, das beispielsweise von SETool unterstützt wird; ebenfalls ein Flasher-Tool, das auf JTAG-Basis arbeitet. Somit war sowohl das Vorhandensein der JTAG Pins als auch ihre Lokalisation auf dem Motherboard[45] sicher (siehe Abbildung 13). Anders als das LT30p schaltet sich dieses Modell bei eingelegter Batterie mit zusätzlicher Stromversorgung selbst ein, egal ob diese über eine Steckdose oder den Laptop bereitgestellt wird.

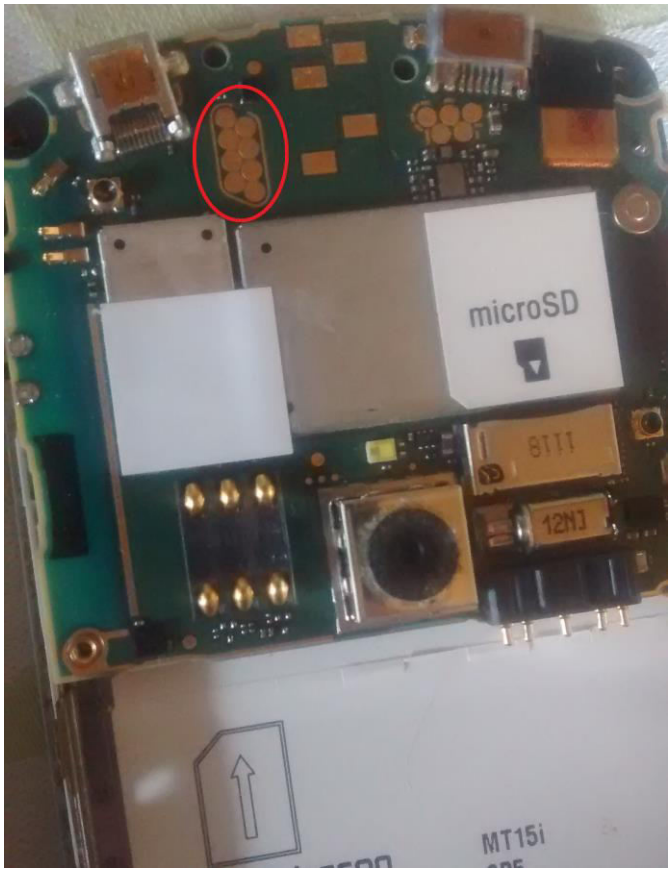

Abbildung 13 Sony Xperia Neo MT15i zerlegt, JTAG Pins hervorgehoben

[45] vgl. http://www.cellcorner.com/xshp/unlock-phone-codes/sony-ericsson-neo-play-arc-tes-point-unlocking-cable-setool.html, unter Detailed Images, 20.08.2017

An der Anzeige im JTAGManager änderte sich aber trotzdem beim Berühren der Pads mit der Nadel nichts.
Als nächstes wurde das Problem der Virtualisierung in Betracht gezogen. Die RIFF Box Software arbeitete in diesem Aufbau in einer Windows 10 virtuellen Maschine unter VMWare Player. Ein fehlerhaftes oder für die RIFF Box nicht geeignetes Weiterleiten der RIFF Box Hardware hätte unter Umständen zu der sinnfreien Anzeige führen können, obwohl die RIFF Box, wie zur Anmeldung am entsprechenden Server und damit der Verwendung des Tools nötig, von der Software erkannt wurde.
Um auch eine Störung der RIFF Box Software durch eventuell durch mehrjährige Nutzung des verwendeten Laptops hervorgerufene Veränderungen am Hostsystem auszuschließen, wurde der JTAGManager inklusive Treiber auch ohne Verwendung von Virtualisierungssoftware direkt auf einem Windows 8 Computer installiert, die Box angeschlossen und angemeldet.
Da auf diesem Rechner die selbe Anzeige mit den selben absurden Werten zu sehen war, wurden auch diese beiden Faktoren als Ursachen ausgeschlossen.
Theoretisch hätte das zum Probing verwendete Kabel nicht funktionsfähig sein können, was aber die abstrusen Werte in der Anzeige ebenfalls nicht erklärt hätte, sondern lediglich als Ursache für das Fehlen der korrekten Werte infrage käme.
Damit lag ein Fehler seitens der RIFF Box nahe. Diese wurde nun mithilfe eines Oszillators auf allgemeine Tauglichkeit getestet. Die anderen Funktionen der RIFF Box scheinen fehlerfrei einsetzbar zu sein.
Zusätzlich wurde der für das Probing verwendete, in der RIFF Box verbaute Widerstand von 10k (siehe Abbildung 14, im rechten unteren Bildbereich) auf Funktion getestet und konnte ebenfalls als Fehlerquelle ausgeschlossen werden.

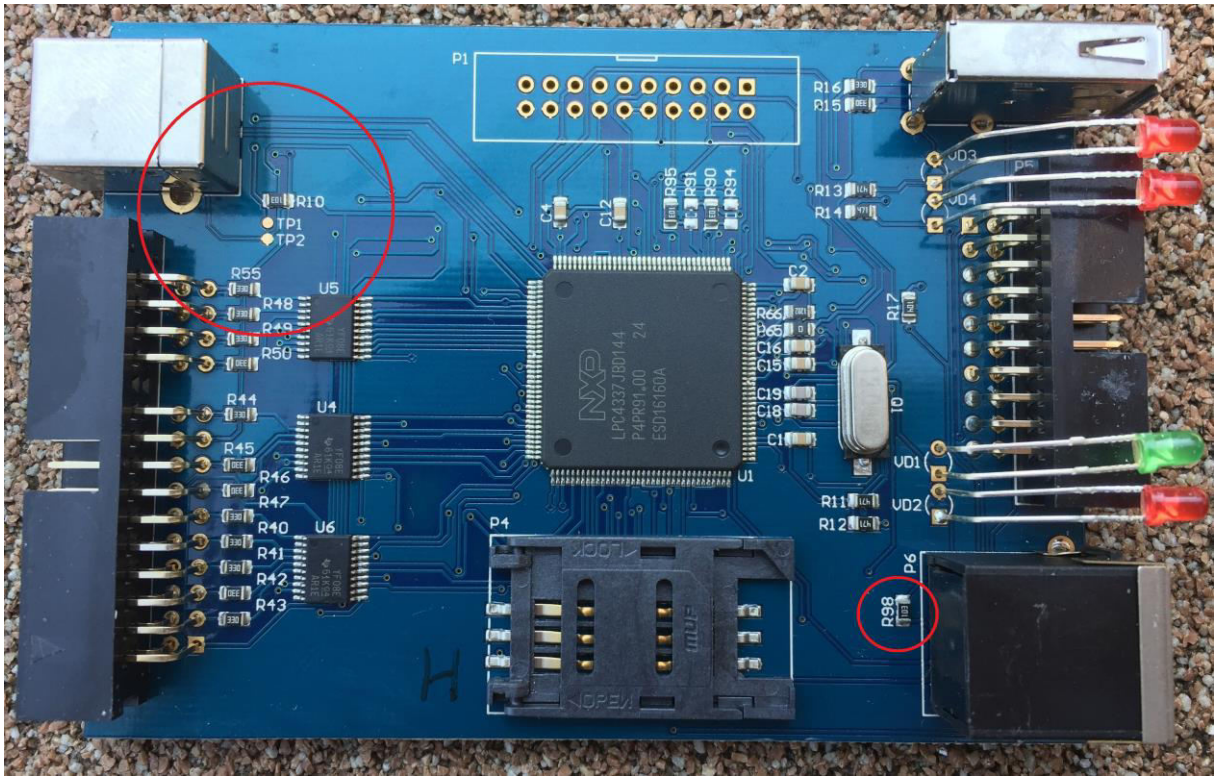

Abbildung 14 Hardware RIFF Box[46]

Das macht einen Fehler in der von der Box für das Probing verwendeten Software wahrscheinlich.
Grundsätzlich wäre die Zuordnung der JTAG Pins TDO, TRST, RTCK und NRST auch manuell möglich, da dafür lediglich die, aus der über einen Widerstand (hier 10k) angelegte Spannung resultierende, Spannung gemessen und die Ergebnisse entsprechend interpretiert werden müssen.
Ein JTAG Pin kann dabei ein Eingang mit oder ohne Pull-up Widerstand oder ein Ausgang sein.
Befindet sich ein Ausgang allerdings im Z-State, wie TDO, verhält er sich wie ein Eingang mit extrem hohem Eingangswiderstand. Dann ist die resultierende Spannung gleich der jeweils Angelegten.
Bei TRST handelt es sich um einen Eingang ohne Pull-up, so das ohne angelegte Spannung auch keine resultiert und eine angelegte Spannung durch den Eingangswiderstand abfällt.
Das RTCK Signal lässt sich durch die bei beiden Tests sehr niedrigen gemessenen Werte vergleichsweise leicht identifizieren. RTCK ist ein Ausgang mit logischem 0 Pegel.[47]

---

[46] vgl. http://www.riffbox.org/wp-content/uploads/2017/04/TP.jpg, 09.09.2017, mit Hervorhebung des genannten Widerstands, zum Vergleich siehe Abbildung 5

[47] Als knappe Hintergrundinformation dazu auch : http://www.elektronik-kompendium.de/sites/dig/0205171.htm, 07.09.2017

NRST ist ein Eingang mit sehr starkem Pull-up, so dass die resultierenden Werte ohne angelegte Spannung auffallend hoch sind. Damit ist auch die Zuordnung dieses Pins verhältnismäßig simpel. Ist dieser Pull-up extrem stark, kann das Signal sich sogar wie ein Ausgang mit logischem 1 Pegel verhalten, also sowohl ohne als auch mit angelegter Spannung eine eher hohe, in beiden Fällen annährend gleiche, resultierende Spannung ergeben.[48] Anschließend müssten, wie auch unter Nutzung der RIFF Box, TDI, TMS und TCK durch Ausprobieren identifiziert werden, was manuell aufgrund der annährend gleichen Ergebnisse eventuell problematisch sein könnte. Hierzu ließe sich allerdings trotzdem die RIFF Box verwenden, das Analysieren der JTAG-Kette ist eine der korrekt arbeitenden Funktionen derselben.
In einer 2007 von Breeuwsma et al. veröffentlichten Arbeit setzen sich die Autoren unter Anderem damit auseinander, wie ein potentieller Ermittler auf einem PCB[49] eine eventuelle JTAG-Schnittstelle finden kann. Es werden unterschiedliche Vorgehensweisen kurz beschrieben. Eine Möglichkeit wäre das Ablöten des Prozessors eines Referenzsystems, das dabei höchstwahrscheinlich funktionsunfähig wird. Dann können die Traces auf dem PCB mittels Multi-Meters gemessen und darüber die JTAG-Schnittstelle gefunden werden. Theoretisch wäre auch die Verwendung eines Röntgen-Geräts zur Ermittlung des JTAG TAP bei einem Multilayer PCB möglich. Als dritte Methode wird das Messen an allen infrage kommenden Pads genannt, gefolgt von einer zweiten Messung, diesmal allen aus den restlichen Pads möglichen Input / Output Kombinationen, bis ein valides Signal erkannt wird.[50]
Außerdem bietet die Easy-JTAG Box ebenfalls eine Anwendung, die die wichtigsten JTAG Pins (TDI, TDO, TMS, TCK, TRST) zuordnen kann.[51] Zudem ist auch ein JTAG Finder im Internet erhältlich, der scheinbar die gleiche Aufgabe erfüllt.[52]
Auf Pinfinder nehmen die Hersteller der RIFF Box im Probing Manual Bezug, indem sie ihre Version aufgrund des bereits verbauten 10k Widerstandes für sicherer erklären, ohne das Vergleichsobjekt genauer zu benennen.[53]
Selbst wenn das Probing Feature ordnungsgemäß funktionieren würde, wäre es sinnvoll, den Aufwand gegen den Nutzen abzuwägen.
Zunächst ist dazu festzustellen, dass, auch wenn im Internet bisweilen gegensätzliches behauptet wird[54], nicht alle Smartphones JTAG unterstützen.[55] Das Probing wäre dem-

[48] vgl. RIFF Probing Manual, http://www.riffbox.org/downloads/manuals/, JTAG_Signals_Probing.pdf, 12.04.2017

[49] printed circuit board

[50] Breeuwsma, Marcel, de Jongh, Martien, Klaver, Coert, van der Knijff, Ronald, Roeloffs, Mark: Forensic Data Recovery from Flash Memory, Small Scale Digital Device Forensics Journal, VOL. 1, NO. 1, JUNE 2007, S.5

[51] vgl. http://z3x-team.com/easy-jtag-activation/, 09.09.2017

[52] vgl. http://jtagfinder.com/x/, 09.09.2017

[53] vgl. JTAG_Signals_Probing.pdf, 2010

[54] vgl. Forensische Datenwiederherstellung mittels Chip-Off und JTAG, 2016, URL : https://www.cwit.de/forensische-datenwiederherstellung-mittels-chip-off-und-jtag/ , 11.09.2017
Hier wird festgestellt, dass „Sämtliche modernen IT-Endgeräte, aber auch andere Elektrogeräte [...] über eine JTAG-Schnittstelle“ verfügen.

[55] vgl. Seung Jei Jang, Jung HoChoi, Ki BomKim, TaejooChang: New acquisition method based on firmware update protocols for Android smartphones, DFRWS, p.68-76, 2015, S.69

nach ohnehin nur für solche Mobiltelefone geeignet, die einerseits JTAG-fähig sind andererseits noch nicht von der RIFF Box unterstützt werden.
Außerdem ist nicht sicher, ob die RIFF Box nach erfolgreicher Durchführung des Probing, das vom Hersteller nur für unterstützte Prozessoren gedacht ist, in der Lage wäre, ein korrektes Abbild des Speichers zu erstellen. Dies könnte zum Beispiel nur bei Geräten mit unterstütztem Prozessor und Speichercontroller tatsächlich möglich sein, was die Anzahl an Geräten, bei denen dieses Vorgehen sinnvoll zur Anwendung kommen könnte, unter Umständen weiter eingrenzt.
Sollte dem aber nicht so sein, wäre sogar eine potentielle Sicherung anderer Endgeräte wie GPS Navigationsgeräten in Betracht zu ziehen und eventuell näher zu untersuchen. Zum Beispiel haben Roeloffs und van Eijk 2010 mittels JTAG den RAM und damit volatile Daten eines TomTom GPS Navigationsgerätes extrahiert.[56]
Zudem ist eine Datensicherung via JTAG vergleichsweise langsam[57] und im Falle einer kompletten Festplattenverschlüsselung nutzlos, sofern nicht Schlüssel und verwendeter Algorithmus bekannt sind.[58]
Die Zeit, die das Erstellen eines vollständigen Abbildes mit der RIFF Box und dem JTAG Manager in Anspruch nimmt, ist im Größenverhältnis von knapp vier Stunden pro Gigabyte anzusetzen.[59]
Laut Venkateswara und Chakravarthy können bei einer Sicherung mittels JTAG auch vergleichsweise eher wenige Daten ausgewertet werden (siehe Abbildung 15).

	Andriller	Paraben mobile forensics tools	JTAG	Chip-Off Acquisition	Whatsapp Xtract
Root required	Ja	Nein	Nein	Nein	Ja
Call logs	Ja	Ja	Ja	Ja	Nein
SMS/MMS	Ja	Ja	Ja	Ja	Nein
Contacts	Ja	Ja	Ja	Ja	Nein
Browser History	Ja	Ja	Ja	Ja	Nein
Gallery	Ja	Ja	Ja	Ja	Nein
Device In-	Ja	Ja	Nein	Nein	Nein

[56] vgl. van Eijk, Onno, Roeloffs, Mark : Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems, in Digital Investigation, S.179-188, 2010

[57] vgl. Seung Jei Jang, Jung HoChoi, Ki BomKim, TaejooChang: New acquisition method based on firmware update protocols for Android smartphones, DFRWS, p.68-76, 2015, S.69

[58] Venkateswara Rao V., A. S. N. Chakravarthy: Survey on Android Forensic Tools and Methodologies, International Journal of Computer Applications, 2016

[59] vgl. Kong, Yu Cho: A Forensic Analysis Approach to Smartphones from a criminal investigation perspektive, 2015, S.80

formation					
Whatsapp messages	Ja	Nein	Nein	Ja	Ja
Skype messages	Ja	Nein	Nein	Ja	Nein
Viber messages	Ja	Nein	Nein	Ja	Nein
Hike messages	Ja	Nein	Nein	Ja	Nein
App related information	Ja	Ja	Nein	Nein	Nein
Malicious Apps Analysis	nein	Nein	Nein	Nein	Nein
Deleted data	Ja	Ja	Ja	Nein	Nein
Recovery of data	Ja	Ja	Ja	Nein	Nein
Presentation	Ja	Ja	Nein	Nein	Nein

Abbildung 15: Vergleich unterschiedlicher Forensiktools (Abschrift)[60]

Demnach kann bei einer Auswertung von über JTAG erlangten Daten auf das Anrufprotokoll, SMS/MMS, Kontakte, Browserverlauf, in der Galerie gespeicherte Bilder und gelöschte Daten zugegriffen werden. Geräteinformationen, Whatsapp/Skype/Viber/Hike-Nachrichten und App bezogene Daten können allerdings nicht dargestellt werden.
Dabei sollte berücksichtigt werden, dass für das Auswerten von über JTAG gesicherten Daten unterschiedliche Software genutzt werden kann. Das hier ebenfalls vorgestellte Tool Paraben mobile forensic tools bietet zum Beispiel zusätzlich zur logischen auch eine physikalische Sicherung mittels JTAG an, ist dabei sogar mit einem mit der RIFF Box erstellten Memory Dump kompatibel. Paraben ist im Vergleich zu JTAG fähig, Geräteinformationen und App bezogene Daten zu sichern und ist JTAG auch in Sachen Präsentation überlegen, möglicherweise aufgrund von zusätzlichen logischen Sicherungen (siehe Abbildung 15).
Leider erwähnen die Autoren nicht, ob die Mängel software- oder sicherungsbedingt sind. Da zum Beispiel bei der Chip-Off Forensik ein vollständiges Abbild der Daten des Speicherchips erstellt wird, macht es wenig Sinn, dass bei dieser Methode, wie in Ab-

[60] Venkateswara Rao V., A. S. N. Chakravarthy: Survey on Android Forensic Tools and Methodologies, International Journal of Computer Applications, 2016

bildung 15 aufgeführt, gelöschte Daten nicht sichergestellt werden können. Es wäre also denkbar, dass sich diese Schwäche lediglich auf die für die Bewertung herangezogene Software zur Präsentation der gesicherten Daten bezieht und nicht auf die Methode selbst.
In einer Studie von 2013 haben Wissenschaftler der Korea University beziehungsweise des University College Dublin die unter Ausnutzen des Recovery Mode gesicherten Nutzerdaten per Hashwert mit durch JTAG erlangten Daten der selben Smartphones verglichen und sind zu dem Schluss gekommen, dass beide Varianten Datenintegrität garantieren.[61]
In einer Arbeit aus dem selben Jahr wird JTAG von Vasa trotz einiger Vorteile als nicht-forensische Methode beschrieben, die die Datenintegrität der Ergebnisse nicht gewährleisten kann.[62]
Bereits 2004 wurde von Eberle, Gura[63] und Wander[64] eine verbindungslose Version des JTAG Standards für Systeme mit mehreren Platinen vorgestellt[65], ein Gedanke, der, zumindest in Bezug auf das Testen von integrierten Schaltungen, 2006[66] und 2007[67] aufgegriffen und verwendet wurde. Das würde zumindest das Risiko, das betreffende Gerät eventuell zu beschädigen, verringern.
Zugleich könnte das ein weiteres Gefahrenpotential betonen:
JTAG gewährt Zugriff auf unterschiedliche Test-Modi, von denen einige von den Herstellern kaum bis gar nicht dokumentiert sind. Ein Reverse Engineering dieser Modi ist aber, nach Ermittlung der JTAG Pins, durchaus möglich und könnte Hackern „Back Door“ Zugriff verschaffen.[68]
Besonders in Kombination mit der Möglichkeit der Verbindungslosigkeit zeigt das aus forensischem Blickwinkel sowohl ein Risikopotential als auch eine eventuelle Chance, die bedacht werden sollten.

---

[61] vgl. Son, Namheun, Lee, Yunho, Kim, Dohyun, James, Joshua I., Lee, Sangjin, Lee, Kyungho: A study of user data integrity during acquisition of Android devices, in: Digital Investigation 10, S.3-11, 2013

[62] vgl. Vasa, Toma S.: Mobile Phone: Identifying Configuration Signatures of Local Devices Absent from XRY, 2013, S.30f.

[63] beide von Sun Microsystems Laboratoies

[64] von der University of Michigan, Ann Arbor

[65] vgl. Eberle, Hans, Gura, Nils, Wander, Arvinderpal: Testing Systems Wirelessly, VLSI Test Symposium, 2004. Proceedings. 22nd IEEE

[66] vgl. Serge Bernard, David Andreu, Marie-Lise Flottes, Philippe Cauvet, Hervé Fleury, et al. : Testing System-In-Package Wirelessly. IEEE. DTIS: Design and Technology of Integrated Systems in Nanoscale Era, Sep 2006, Tunis, Tunisia. Design and Technology of Integrated Systems in Nanoscale Era, pp.222-226, 2006.

[67] vgl. Moore, B., Sellathamby, C., Cauvet, P., Fleury, H., Paulson, M., Reja, M., Fu, L., Bai, B., Reid, E., Filanovsky, I., Slupsky, S.: High Throughput Non-contact SiP Testing, International Test conference, 2007

[68] vgl. Domke, Felix: Blackbox JTAG Reverse Engineering, 2009, S.1, 5

Gerade durch die Entwicklung von Smartphones von mobilen Telefonen zu mobilen Computern mit zahlreichen personenbezogenen Daten wie Standorten oder Kontoinformationen erhöht den Bedarf an Sicherheit dieser Geräte.[69]

4.2 Fazit

Das hier betrachtete Feature ist, wie im Rahmen der Diskussion erläutert, nicht zwangsläufig nötig, um die JTAG Pins nicht unterstützter Geräte zuzuordnen. Zum Einen gibt es andere Tools, die diese Anwendung anbieten, zum Anderen wäre eine Bestimmung auch manuell durchführbar.
Auch lässt sich die Menge der Geräte, für die dieses Vorgehen zur Datensicherung infrage käme, schlecht bestimmen, scheint aber eher eine vergleichsweise kleine Anzahl an Smartphones zu sein.
Da das Feature zumindest aktuell einen vermutlichen Softwarefehler hat, kann es natürlich ohnehin nicht verwendet werden.
Sollte dieser Fehler behoben werden, handelt es sich vermutlich um ein verhältnismäßig unkompliziertes Verfahren, das auch ohne großes Hintergrundwissen durchgeführt werden können und eine nachfolgende Datensicherung passender Smartphones, eventuell auch anderer Endgeräte, möglich machen sollte.

4.3 Schluss

Venkateswara und Chakravarthy, den Verfassern von Survey on Android Forensic Tools and Methodologies im International Journal of Computer Applications, zufolge ist es aufgrund der überaus schnellen Weiterverbreitung von Android Systemen für die digitale Forensik unabdingbar, ein standardisiertes Vorgehen zur kriminaltechnischen Sicherung und Untersuchung von Smartphones, Tablets oder anderen Geräten, die dieses Betriebssystem nutzen, zu entwickeln.[70] Leider ist dies gerade aufgrund der enorm hohen Anzahl unterschiedlichster Hardware, Dateisysteme und deren Kombinationen beinahe unmöglich.[71]

---

[69] vgl. IT-forensische Smartphone-Analyse | mobile Forensik
URL: https://www.it-forensik-it-sicherheit.de/it-forensik/kriminalistische-it-forensik/smartphone-forensik/, 13.09.2017

[70] vgl. Venkateswara Rao V., A. S. N. Chakravarthy: Survey on Android Forensic Tools and Methodologies, International Journal of Computer Applications, 2016

[71] vgl. Mobile IT-Forensik / Mobile Endgeräteauswertung: Auswertung von Mobiltelefon & Smartphone, URL: http://www.lressmann.de/edvitbewertungsgutachter/mobile-forensik.htm, 14.09.2017

Bereits 2014 waren laut einer Studie von Open Signal allein knapp 19000 unterschiedliche Android-Modelle auf dem Markt.[72]
Statistisch betrachtet besitzen heute über 60% der Bevölkerung ein Mobiltelefon.[73]
Allein 2016 wurden einer Studie von gfu Consumer & Home Electronics zufolge nur in Deutschland 23,2 Millionen Smartphones an Privatkunden verkauft.[74]
Diese Zahlen belegen, wie wichtig der Bereich der Mobilfunkforensik heutzutage ist und wie bedeutend er in Zukunft noch werden könnte.

[72] vgl. Kling, Bernd: Auswahl von Android-Smartphones steigt auf knapp 19.000 Modelle, 2014, URL: http://www.zdnet.de/88203257/auswahl-von-android-smartphones-steigt-auf-knapp-19-000-modelle/, 19.10.2016

[73] vgl. Mobile IT-Forensik / Mobile Endgeräteauswertung: Auswertung von Mobiltelefon & Smartphone, URL: http://www.lressmann.de/edvitbewertungsgutachter/mobile-forensik.htm, 14.09.2017

[74] vgl. http://www.gfu.de/fileadmin/media/downloads/Infografiken-gfu-Smartphones-2017.jpg, 15.09.2017

Literaturverzeichnis

Breeuwsma, Marcel, de Jongh, Martien, Klaver, Coert, van der Knijff, Ronald, Roeloffs, Mark: Forensic Data Recovery from Flash Memory, 2007

Domke, Felix: Blackbox JTAG Reverse Engineering, 2009

Eberle, Hans, Gura, Nils, Wander, Arvinderpal: Testing Systems Wirelessly, VLSI Test Symposium, 2004

van Eijk, Onno, Roeloffs, Mark : Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems, in Digital Investigation, S.179-188, 2010

Keonwoo Kim, Dowon Hong, Kyoil Chung, and Jae-Cheol Ryou: Data Acquisition from Cell Phone using Logical Approach, in: Proceedings of world academy of science, engineering and technology, 2007

Kong, Yu Cho: A Forensic Analysis Approach to Smartphones from a criminal investigation perspektive, 2015

Moore, B., Sellathamby, C., Cauvet, P., Fleury, H., Paulson, M., Reja, M., Fu, L., Bai, B., Reid, E., Filanovsky, I., Slupsky, S.: High Throughput Non-contact SiP Testing, International Test conference, 2007

Mylonas, Alexios: Security and Privacy in Ubiquitous Computing: The Smart Mobile Equipment Case, 2013

Mylonas et al.: Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition, 2011

Serge Bernard, David Andreu, Marie-Lise Flottes, Philippe Cauvet, Hervé Fleury, et al. : Testing System-In-Package Wirelessly. IEEE. DTIS: Design and Technology of Integrated Systems in Nanoscale Era, Sep 2006, Tunis, Tunisia. Design and Technology of Integrated Systems in Nanoscale Era, pp.222-226, 2006

Seung Jei Jang, Jung HoChoi, Ki BomKim, TaejooChang: New acquisition method based on firmware update protocols for Android smartphones, DFRWS, p.68-76, 2015

Son, Namheun, Lee, Yunho, Kim, Dohyun, James, Joshua I., Lee, Sangjin, Lee, Kyungho: A study of user data integrity during acquisition of Android devices, in: Digital Investigation 10, S.3-11, 2013

Vasa, Toma S.: Mobile Phone: Identifying Configuration Signatures of Local Devices Absent from XRY, 2013

Venkateswara Rao V., A. S. N. Chakravarthy: Survey on Android Forensic Tools and-Methodologies, International Journal of Computer Applications, 2016

Yung Anh Le:Windows Phone 7 : Implications For Digital Forensic Investigators, 2012

Websites

Forensische Datenwiederherstellung mittels Chip-Off und JTAG, 2016, URL : https://www.cwit.de/forensische-datenwiederherstellung-mittels-chip-off-und-jtag/

Günther, Stephan: JTAG-Interface, Überblick über Aufbau, Funktion und Nutzung, URL: https://tudresden.de/ing/informatik/ti/vlsi/ressourcen/dateien/dateien_studium/dateien_lehstuhlseminar/vortraege_lehrstuhlseminar/hs_ws_0708/jtag-schnittstelle.pdf?lang=de

Heinfling, Benjamin: Ice Cream Sandwich statt Wodka Martini, 2012, URL: http://www.chip.de/artikel/Sony-Xperia_T-Handy-Test_57975160.html

Heinz, Benedikt : Hardware-Debugschnittstelle JTAG auslesen, Linux-Magazin, 2010, URL: http://www.linux-magazin.de/Ausgaben/2010/06/Diagnosewerkzeug

Hoffman, Chris: How To Convert Virtual Machines Between VirtualBox and Vmware, 2012, URL: https://www.howtogeek.com/125640/how-to-convert-virtual-machines-betweenvirtualbox-and-vmware/

IT-forensische Smartphone-Analyse | mobile Forensik URL: https://www.it-forensik-it-sicherheit.de/it-forensik/kriminalistische-itforensik/smartphone-forensik/

Kling, Bernd: Auswahl von Android-Smartphones steigt auf knapp 19.000 Modelle, 2014, URL: http://www.zdnet.de/88203257/auswahl-von-android-smartphones-steigt-auf-knapp-19-000-modelle/

Mobile IT-Forensik / Mobile Endgeräteauswertung: Auswertung von Mobiltelefon & Smartphone, URL: http://www.lressmann.de/edvitbewertungsgutachter/mobile-forensik.htm

Muth, Denise: Leitfaden zur forensischen Untersuchung von Android-Smartphones, 2013, S.63, URL: https://www.dasec.h-da.de/wp-content/uploads/2013/08/muth-denisemasterarbeit-ss131.pdf

RIFF JTAG Features, URL : http://www.riffbox.org/category/riff-jtag-features/,

RIFF Box Getting Started, URL: https://www.riffbox.org/category/jtag-support/

RIFF JTAG Manager v1.67, RIFF Box Firmware v1.43, 2017, URL: https://www.riffbox.org/jtag-news/riff-jtag-manager-v1-67-riff-box-firmware-v1-43/

RIFF Box Probing Manual, URL : http://www.riffbox.org/downloads/manuals/JTAG_Signals_Probing.pdf, 2010

RIFF Box User Manual, URL: https://www.riffbox.org/category/jtag-support/

Schonschek, Oliver: Digitale Spurensuche auf Smartphones: Tools für die mobile Forensik, 2013, URL: https://www.computerwoche.de/a/tools-fuer-die-mobile-forensik,2533050

http://ark.intel.com/de/products/50176/Intel-Pentium-Processor-P6200-3M-Cache-2_13-GHz

http://www.askingbox.de/frage/virtualbox-unterschied-zwischen-ova-und-ovf-datei

http://www.cellcorner.com/xshp/unlock-phone-codes/sony-ericsson-neo-play-arc-tes-pointunlocking-cable-setool.html

http://www.elektronik-kompendium.de/sites/dig/0205171.htm

https://www.fonefunshop.com/Probe-Cable-For-Riff-Box.html

http://www.gfu.de/fileadmin/media/downloads/Infografiken-gfu-Smartphones-2017.jpg

http://jtagfinder.com/x/

https://www.riffbox.org/tag/pins/

http://www.riffbox.org/wp-content/uploads/2017/04/TP.jpg

https://de.wikipedia.org/wiki/Open_circuit#Pull-up

https://www.xjtag.com/about-jtag/jtag-a-technical-overview/

https://www.youtube.com/watch?v=luRdICkdkx8

https://www.youtube.com/watch?v=4BtXZiVLtWc

http://z3x-team.com/easy-jtag-activation/

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ort, Datum Vorname Nachname